What is claimed is:

1. An information management system comprising:

a plurality of workstations adapted for connection to a computer network, each workstation having a memory;

a data repository arranged to receive data from each of said workstations;

an application stored in said memory of each workstation for transmitting outbound data to said network and receiving inbound data from said network;

policy data containing rules defining relevant data which is to be stored in said data repository; and

an analyser, said analyser being operable in conjunction with said policy data to monitor at least one of said outbound data and said inbound data, to identify in at least one of said outbound data and said inbound data, relevant data that is to be stored in said data repository in accordance with said rules in said policy data, and to cause said relevant data to be stored in said data repository.

2. The system of claim 1 wherein said relevant data that is to be stored in said data repository is encrypted prior to it being transmitted to said data repository.

3. The system of claim 1 wherein said relevant data that is stored in said data repository is encrypted.

4. The system of claim 1 wherein said computer network, to which said one or more workstations are adapted for connection, is the Internet.

5. The system of claim 4 wherein said analyser is operable to identify, as relevant data, at least one of

usernames and passwords used to identify a user, and usernames and passwords used to access web pages on the Internet, and the URL address of the web page at which those usernames and passwords are used,

said identified usernames, passwords and said identified URLs being stored in said data repository.

6. The system of claim 5 wherein said analyser is operable to identify usernames and passwords from the field names of data contained in at least one of said outbound data and said inbound data.

7. The system of claim 5 wherein a representation of the input fields of a web page is stored in said memory of said one or more workstations, and wherein said analyser is operable to identify usernames and passwords from said representation.

8. The system of claim 5 wherein said analyser is operable to identify usernames or passwords from the field types of data contained in said outbound or said inbound data.

9. The system of claim 4 wherein said analyser is operable to identify, as relevant data, digital certificates contained in at least one of said outbound or said inbound data or used to digitally sign signed data in said inbound data or said outbound data, or sufficient descriptive data to identify such digital certificates,

said digital certificates and/or said descriptive data being stored in said data repository.

10. The system of claim 9 wherein said analyser is operable to identify one or more of the following data as relevant data:

whether or not said digital certificate has been revoked;

the identity of the holder of said digital certificate;

the amount of any eCommerce transaction being made that is related to said digital certificate;

the goods or services being sold in any eCommerce transaction being made with said digital certificate;

the date of receipt of said digital certificate;

and wherein said identified data is stored with said digital certificate in said data repository.

11. The system of claim 4 wherein the analyser is operable to identify when an eCommerce transaction is occurring and if an eCommerce transaction is identified as occurring, to identify in said outbound or said inbound data one or more of the following data as relevant data:

the URL address or e-mail address of the remote location to which outbound data is being transmitted or inbound data is being received;

the web pages accessed by a user of said one or more workstations during the transaction;

the amount of the transaction;

the goods or services being traded in the transaction;

the date of the transaction; and

wherein said relevant data is stored in said data repository.

12. The system of claim 1 wherein said analyser is located on each of said one or more workstations.

13. The system of claim 1 wherein said application is a web browser.

14. The system of claim 13 wherein said analyser is a plug-in module of said web browser.

15. The system of claim 14 wherein said web browser is Microsoft's Internet Explorer and said analyser is a Browser Helper Object.

16. The system of claim 1 wherein said application is an e-mail client.

17. The system of claim 16 wherein said analyser is a plug-in module of said e-mail client.

18. The system of claim 17 wherein said e-mail client is Microsoft's Outlook e-mail client and said analyser is a Microsoft Exchange client extension.

19. The system of claim 1 wherein said network includes a server and said analyser is located at a point on said network intermediate said one or more workstations and said server, or said analyser is located at said server.

20. The system of claim 1 further comprising a supervisor workstation, said supervisor workstation having access to said data repository and being operable to view said relevant data stored in said data repository.

21. The system of claim 20 wherein said policy data is accessible by said supervisor workstation, such that a user of said supervisor workstation can edit said policy data.

22. The system of claim 1 wherein a workstation of said plurality of workstations has access to said data repository and is operable to view said relevant data stored in said data repository.

23. The system of claim 1 wherein said computer network to which said one or more workstations are adapted for connection is a public computer network, and wherein

said one or more workstations together form a private computer network.

24. A method of managing information comprising the steps of:

providing a plurality of workstations adapted for connection to a computer network, each workstation having a memory;

providing a data repository arranged to receive data from each of said workstations;

providing an application stored in said memory of each workstation for transmitting outbound data to said network and receiving inbound data from said network;

providing policy data containing rules defining relevant data which is to be stored in said data repository; and

analysing at least one of said outbound data and said inbound data, with reference to said policy data, to identify in at least one of said outbound data and said inbound data, relevant data that is to be stored in said data repository in accordance with said rules in said policy data; and

storing said relevant data in said data repository.

25. The method of claim 24 further comprising the step of encrypting said relevant data that is to be stored in said data repository prior to it being stored in said data repository.

26. The method of claim 24 further comprising the step of encrypting said relevant data that is stored in said data repository after it has been stored in said data repository.

27. The method of claim 24 wherein said computer network, to which said one or more workstations are adapted for connection, is the Internet.

28. The method of claim 27 wherein in the analysing step, at least one of usernames and passwords used to identify a user, and usernames and passwords used access web pages on the Internet, and the URL address of those web pages, are identified as relevant data.

29. The method of claim 28 wherein in said analysing step, usernames and passwords are identified from the field names of data contained in at least one of said outbound data and said inbound data.

30. The method of claim 28 wherein a representation of the input fields of a web page is stored in said memory of said one or more workstations, and wherein in said analysing step usernames and passwords are identified from said representation.

31. The method of claim 28 wherein in said analysing step usernames or passwords are identified from the field types of data contained in said outbound or said inbound data.

32. The method of claim 27 wherein in said analysing step, digital certificates contained in at least one of said outbound or said inbound data or used to digitally sign signed data in said inbound or said outbound data, are identified as relevant data, or sufficient descriptive data to identify such digital certificates, is identified as relevant data.

33. The method of claim 32 wherein said analysing step includes identifying one or more of the following data as relevant data:

whether or not said digital certificate has been revoked;

the identity of the holder of said digital certificate;

the amount of any eCommerce transaction being made that is related to said digital certificate;

the goods or services being sold in any eCommerce transaction being made with said digital certificate; and

the date of receipt of said digital certificate.

34. The method of claim 27 wherein said analysing step includes identifying when an eCommerce transaction is occurring and if an on-line eCommerce transaction is identified as occurring, identifying in said outbound or said inbound data one or more of the following data as relevant data:

the URL address or e-mail address of the remote location to which outbound data is being transmitted or inbound data is being received;

the web pages accessed by a user of said one or more workstations during the transaction;

the amount of the transaction;

the goods or services being traded in the transaction;

the date of the transaction.

35. The method of claim 24 wherein said analysing step is carried out at said one or more workstations.

36. The method of claim 24 wherein said application is a web browser.

37. The method of claim 36 wherein said analysing step is performed by a plug-in module of said web browser.

38. The method of claim 37 wherein said web browser is Microsoft's Internet Explorer and said plug-in module is a Browser Helper Object.

39. The method of claim 24 wherein said application is an e-mail client.

40. The method of claim 39 wherein said analysing step is performed by a plug-in module of said e-mail client.

41. The method of claim 40 wherein said e-mail client is Microsoft's Outlook e-mail client and said plug-in module is a Microsoft Exchange client extension.

42. The method of claim 24 wherein said network includes a server and said analysing step is performed at a point on said network intermediate said one or more workstations and said server, or said analysing step is performed at said server.

43. The method of claim 24 further comprising the step of providing a supervisor workstation, said supervisor workstation having access to said data repository and being operable to view said relevant data stored in said data repository.

44. The method of claim 43 wherein said policy data is accessible by said supervisor workstation, such that a user of said supervisor workstation can edit said policy data.

45. The method of claim 24 wherein a workstation of said plurality of workstations has access to said

data repository and is operable to view said relevant data stored in said data repository.

46. The method of claim 24 wherein said computer network to which said one or more workstations are adapted for connection is a public computer network, and wherein said one or more workstations together form a private computer network.

47. A computer program product, for controlling a plurality of computers in a private network to manage information, the network having a data repository arranged to receive data from the plurality of computers and policy data containing rules defining relevant data which is to be extracted from at least one of outbound data transmitted to a public network or inbound data received from the public network and stored in the data repository, comprising:

a recording medium readable by the computer, having program code recorded thereon which when executed on each of said plurality of computers, configures said computers to:

analyse, in conjunction with an application running on each of said computers that is operable to transmit the outbound data and receive the inbound data, at least one of said outbound data and said inbound data, with reference to said policy data, to identify in at least one of said outbound data and said inbound data, relevant data that is to be stored in said data repository in accordance with said rules in said policy data; and

cause said relevant data to be stored in said data repository.

48. The computer program product of claim 47 wherein said program code when executed on said computer is operable to cause said relevant data that

is to be stored in said data repository to be encrypted prior to it being stored in said data repository.

49. The computer program product of claim 47 wherein said program code when executed on said computer is operable to cause said relevant data that is stored in said data repository to be encrypted.

50. The computer program product of claim 47 wherein said application is adapted to transmit outbound data to the Internet and receive inbound data from the Internet.

51. The computer program product of claim 50 wherein at least one of usernames and passwords used to identify a user, and usernames and passwords used to access web pages on the Internet, and the URL address of those web pages, are identified as relevant data.

52. The computer program product of claim 51 wherein usernames and passwords are identified from the field names of data contained in at least one of said outbound data and said inbound data.

53. The computer program product of claim 51 wherein a representation of the input fields of a web page is stored in said memory of said one or more workstations, and wherein said usernames and passwords are identified from said representation.

54. The computer program product of claim 51 wherein usernames or passwords are identified from the field types of data contained in said outbound or said inbound data.

55. The computer program product of claim 50 wherein digital certificates contained in at least one of said outbound or said inbound data or used to

digitally sign signed data in said inbound data or said outbound data, or sufficient descriptive data to identify any such digital certificates, are identified as relevant data.

56. The computer program product of claim 55 wherein one or more of the following data are identified as relevant data:

whether or not said digital certificate has been revoked;

the identity of the holder of said digital certificate;

the amount of any eCommerce transaction being made that is related to said digital certificate;

the goods or services being sold in any eCommerce transaction being made with said digital certificate; and

the date of receipt of said digital certificate.

57. The computer program product of claim 50 wherein the program code when executed on said computer is further operable to:

identify when an eCommerce transaction is occurring; and

if an eCommerce transaction is identified as occurring, to identify in said outbound or said inbound data one or more of the following data as relevant data:

the URL address or e-mail address of the remote location to which outbound data is being transmitted or inbound data is being received;

the web pages accessed by a user of said one or more workstations during the transaction;

the amount of the transaction;

the goods or services being traded in the transaction; and

the date of the transaction.

58. The computer program product of claim 47 wherein said program code is executable at each of said computers.

59. The computer program product of claim 47 wherein said application is a web browser.

60. The computer program product of claim 59 wherein said program code when executed on said computer is a plug-in module of said web browser.

61. The computer program product of claim 60 wherein said web browser is Microsoft's Internet Explorer and said plug-in module is a Browser Helper Object.

62. The computer program product of claim 47 wherein said application is an e-mail client.

63. The computer program product of claim 62 wherein said program code when executed on said computer is a plug-in module of said e-mail client.

64. The computer program product of claim 63 wherein said e-mail client is Microsoft's Outlook e-mail client and said plug-in module is a Microsoft Exchange client extension.

65. The computer program product of claim 47 wherein said network includes a server and said program code is executable at a point on said network intermediate said one or more workstations and said server, or said program code is executable at said server.

66. The computer program product of claim 47 further comprising program code recorded on the

recording medium which when executed on a computer in said plurality of computers enables that computer as a supervisor workstation, said supervisor workstation having access to said data repository and being operable to view said relevant data stored in said data repository.

67. The computer program product of claim 66 wherein said policy data is accessible by said supervisor workstation, such that a user of said supervisor workstation can edit said policy data.

68. The computer program product of claim 47 further comprising program code recorded on the recording medium which when executed on a computer in said plurality of computers provides that computer with access to said data repository such that a users of said computer can view said relevant data stored in said data repository.

69. A system for recording passwords and usernames comprising:

a plurality of workstations adapted for connection to the Internet, each workstation having a memory;

a data repository arranged to receive data from each of said workstations;

an application stored in said memory of each workstation for transmitting outbound data and receiving inbound data from the Internet; and/or an application for receiving user input data; and

an analyser, said analyser being operable to monitor at least one of said input data, said outbound data and said inbound data, to identify usernames and passwords contained in said user input data, said outbound data or said inbound data, and to cause said usernames and passwords to be stored in said data repository.

70. The system of claim 69 wherein said analyser is operable to determine whether the usernames and passwords are used to access a web page, and if they are, to identify the URL address of said web page and cause said URL to be stored in said data repository with said usernames and passwords.

71. The system of claim 69 wherein said relevant usernames and passwords data are encrypted prior to being transmitted to said data repository.

72. The system of claim 69 wherein said relevant usernames and passwords that are stored in said data repository are encrypted.

73. The system of claim 69 wherein said analyser is operable to identify said relevant usernames and passwords from the field names of data contained in at least one of said outbound data or said inbound data.

74. The system of claim 69 wherein a representation of the input fields of a web page is stored in said memory of said one or more workstations, and wherein said analyser is operable to identify said relevant usernames and passwords from said representation.

75. The system of claim 69 wherein said analyser is operable to identify said relevant usernames or passwords from the field types of data contained in said outbound or said inbound data.

76. The system of claim 69 wherein said application has a user interface provided with a 'remember password' option which when selected stores input usernames and passwords in memory, and said analyser is operable to identify said relevant

usernames and passwords in said input usernames and passwords stored in memory.

77. The system of claim 69 wherein said analyser is located on each of said one or more workstations.

78. The system of claim 69 wherein said application is a web browser.

79. The system of claim 78 wherein said analyser is a plug-in module of said web browser.

80. The system of claim 79 wherein said web browser is Microsoft's Internet Explorer and said analyser is a Browser Helper Object.

81. The system of claim 69 wherein said network comprises a server and said analyser is located at a point on said network intermediate said one or more workstations and said server, or said analyser is located at said server.

82. The system of claim 69 further comprising a supervisor workstation, said supervisor workstation having access to said data repository and being operable to view said relevant usernames and passwords stored in said data repository.

83. The system of claim 69 wherein a workstation of said plurality of workstations has access to said data repository and is operable to view said relevant usernames and passwords stored in said data repository.

84. A method for recording passwords and usernames comprising the steps of:

providing a plurality of workstations adapted for connection to the Internet, each workstation having a memory;

providing a data repository arranged to receive data from each of said workstations;

providing an application stored in said memory of each workstation for transmitting outbound data and receiving inbound data from the Internet; and/or an application for receiving user input data; and

analysing at least one of said user input data, said outbound data and said inbound data, to identify usernames and passwords; and

causing said usernames and passwords to be stored in said data repository.

85. The method of claim 84 further comprising the steps of determining whether the usernames and passwords are used to access a web page, and if they are, identifying the URL address of said web page, and storing said URL in said data repository with said usernames and passwords.

86. The method of claim 84 further comprising the step of encrypting usernames and passwords prior to being stored in said data repository.

87. The method of claim 84 further comprising the step of encrypting the usernames and passwords that are stored in said data repository.

88. The method of claim 84 wherein in said analysing step usernames and passwords are identified from the field names of data contained in at least one of said outbound data or said inbound data.

89. The method of claim 84 wherein a representation of the input fields of a web page is stored in said memory of said workstation, and wherein in said analyser step usernames and passwords are identified from said representation.

90. The method of claim 84 wherein in said analysing step usernames and passwords are identified from the field types of data contained in said outbound or said inbound data.

91. The method of claim 84 wherein said application has a user interface provided with a 'remember password' option which when selected stores input usernames and passwords in said memory of said one or more workstations, and wherein in said analysing step usernames and passwords are identified from said input usernames and passwords stored in said memory of said one or more workstations.

92. The method of claim 84 wherein said analysing step is performed on said one or more workstations.

93. The method of claim 84 wherein said application is a web browser.

94. The method of claim 93 wherein said analysing step is performed by a plug-in module of said web browser.

95. The method of claim 94 wherein said web browser is Microsoft's Internet Explorer and said plug-in module is a Browser Helper Object.

96. The method of claim 84 wherein said network comprises a server and said analysing step is performed at a point on said network intermediate said one or more workstations and said server, or said analysing step is performed at said server.

97. The method of claim 84 further comprising the step of providing a supervisor workstation, said supervisor workstation having access to said data

repository and being operable to view said relevant usernames and passwords stored in said data repository.

98. The method of claim 84 wherein a computer of said plurality of computers has access to said data repository and is operable to view said relevant usernames and passwords stored in said data repository.

99. A computer program product, for controlling a plurality of computers in a private network to record passwords and usernames, the network having a data repository arranged to receive data from the plurality of computers, said computer program product comprising:

a recording medium readable by the computer, having program code recorded thereon which when executed on each of said plurality of computers, configures said computers to:

analyse, in conjunction with an application running on the computer that is operable to transmit outbound data to the Internet and receive inbound data from the Internet, and/or an application running on the computer for receiving user input data, at least one of said user input data, said outbound data and said inbound data, to identify in at least one of said user input data, said outbound data and said inbound data, relevant data that is to be stored in said data repository; and

control said computer to store said relevant data in said data repository.

100. The computer program product of claim 99 wherein said program code when executed on said computer is further operable to determine whether the usernames and passwords are used to access a web page, and if they are, to identify the URL address of said web page and to direct the computer to store said URL in said data repository with said usernames and passwords.

101. The computer program product of claim 99 wherein said program code when executed on said computer is further operable to cause said usernames and passwords to be encrypted prior to them being stored in said data repository.

102. The computer program product of claim 99 wherein said program code when executed on said computer is further operable to cause said usernames and passwords that are stored in said data repository to be encrypted.

103. The computer program product of claim 99 wherein said program code when executed on said computer is operable to identify usernames and passwords from the field names of data contained in at least one of said outbound data or said inbound data.

104. The computer program product of claim 99 wherein a representation of the input fields of a web page is stored in the memory of said computer, and wherein said program code when executed on said computer is operable to identify usernames and passwords from said representation.

105. The computer program product of claim 99 wherein said program code when executed on said computer is further operable to identify usernames and passwords from the field types of data contained in said outbound or said inbound data.

106. The computer program product of claim 99 wherein said application for receiving user input data has a user interface provided with a 'remember password' option which when selected stores input usernames and passwords in said memory of said computer, and wherein said program code when executed

on said computer is operable to identify usernames and passwords from said input usernames and passwords stored in said memory of said computer.

107. The computer program product of claim 99 wherein said program code is executable at each of said computers.

108. The computer program product of claim 99 wherein said application is a web browser.

109. The computer program product of claim 108 wherein said program code when executed on said computer is a plug-in module of said web browser.

110. The computer program product of claim 109 wherein said web browser is Microsoft's Internet Explorer and said plug-in module is a Browser Helper Object.

111. The computer program product of claim 99 wherein said network comprises a server and said program code is executable at a point on said network intermediate said computer and said server, or said program code is executable at said server.

112. The computer program product of claim 99 further comprising program code which when executed on said computer enables that computer as a supervisor workstation, said supervisor workstation having access to said data repository and being operable to view said relevant usernames and passwords stored in said data repository.

113. The computer program product of claim 99 wherein a computer of said plurality of computers has access to said data repository and is operable to view

said relevant usernames and passwords stored in said data repository.

114. An information management system comprising:

one or more workstations adapted for connection to a computer network, each workstation having a memory;

an application stored in said memory of each workstation for transmitting outbound data to said network and receiving inbound data from said network;

policy data containing rules specifying an appropriate encryption strength for outbound data, the encryption strength depending on the content of the data; and

an analyser, said analyser being operable in conjunction with said policy data to monitor said outbound data and to determine, in accordance with said rules in said policy data, an appropriate encryption strength for the outbound data;

wherein said analyser controls transmission of said outbound data from said application in dependence upon said determination of an appropriate encryption strength.

115. The system of claim 114 wherein said rules in said policy data define confidential data which can not be transmitted, said analyser being operable in conjunction with said policy data to prevent said confidential data being transmitted from said application.

116. The system of claim 114 wherein said analyser is further operable to determine the present encryption strength in use for transmitting said outbound data; and

wherein said analyser controls transmission of said outbound data from said application both in dependence upon said determination of an appropriate

encryption strength and in dependence upon said determination of the present encryption strength in use.

117. The system of claim 116 wherein if the analyser determines that the present encryption strength in use for transmitting outbound data is less than said appropriate encryption strength, then said analyser prevents transmission of said outbound data from said application.

118. The system of claim 116 wherein if the analyser determines that the present encryption strength in use for transmitting outbound data is less than said appropriate encryption strength, then said analyser prevents transmission of said outbound data from said application and controls said application to renegotiate an encryption strength for transmission that is appropriate.

119. The system of claim 116 wherein if the analyser determines that the present encryption strength in use for transmitting outbound data is less than said appropriate encryption strength, then said analyser modifies the outbound data such that the present encryption strength is an appropriate encryption strength for the transmission of the modified outbound data.

120. The system of claim 116 wherein if the analyser determines that the present encryption strength in use for transmitting outbound data is less than said appropriate encryption strength, then said analyser controls said application to notify a user of said application that the encryption strength in use is not sufficient.

121. The system of claim 114 wherein the analyser is further operable to identify credit card numbers in said outbound data.

122. The system of claim 121 wherein the analyser is further operable to distinguish a predetermined set of credit card numbers from other credit card numbers, wherein said rules of said policy data define different appropriate encryption strengths for outbound data containing credit card numbers in the predetermined set than for other credit card numbers.

123. The system of claim 122 wherein said rules of said policy data specify that there is no appropriate encryption strength for a pre-determined set of one or more credit card numbers.

124. The system of claim 114 wherein said analyser is further operable to identify at least one or more of, credit card numbers, account codes, usernames, passwords, names and addresses and other predetermined keywords in the content of said outbound data.

125. The system of claim 114 wherein said rules in said policy data specify an appropriate encryption strength for said outbound data, that is dependent on the address to which said outbound data is to be transmitted.

126. The system of claim 114 wherein said analyser is located on each of said one or more workstations.

127. The system of claim 114 wherein said application is a web browser.

128. The system of claim 127 wherein said analyser is a plug-in module of said web browser.

129. The system of claim 128 wherein said web browser is Microsoft's Internet Explorer and said analyser is a Browser Helper Object.

130. The system of claim 114 wherein said application is an e-mail client.

131. The system of claim 130 wherein said analyser is a plug-in module of said e-mail client.

132. The system of claim 131 wherein said e-mail client is Microsoft's Outlook e-mail client and said analyser is a Microsoft client extension.

133. The system of claim 114 wherein said network comprises a server and said analyser is located at a point on said network intermediate said one or more workstations and said server, or said analyser is located at said server.

134. The system of claim 114 wherein said computer network to which said one or more workstations are adapted for connection is a public computer network, and wherein said one or more workstations together form a private computer network.

135. The system of claim 114 further comprising a supervisor workstation, said policy data being accessible by said supervisor workstation, such that a user of said supervisor workstation can edit said policy data.

136. A method of managing information comprising the steps of:

providing one or more workstations adapted for connection to a computer network, each workstation having a memory;

providing an application stored in said memory of each workstation for transmitting outbound data to said network and receiving inbound data from said network;

providing policy data containing rules specifying an appropriate encryption strength for outbound data, the encryption strength depending on the content of the data; and

analysing said outbound data to determine, in accordance with said rules in said policy data, an appropriate encryption strength for the outbound data;

controlling transmission of said outbound data from said application in dependence upon the determination of an appropriate encryption strength in said analysing step.

137. The method of claim 136 wherein said rules in said policy data define confidential data which cannot be transmitted, and wherein in said controlling step transmission of said confidential data is prevented.

138. The method of claim 136 wherein said analysing step further comprising the step of determining the present encryption strength in use for transmitting said outbound data; and

wherein in said controlling step the transmission of said outbound data from said application is dependent upon both the determination of an appropriate encryption strength and the determination of the present encryption strength in use.

139. The method of claim 138 wherein if it is determined that the present encryption strength in use for transmitting outbound data is less than said appropriate encryption strength, then in said controlling step transmission of said outbound data from said application is prevented.

140. The method of claim 138 wherein if in said analysing step it is determined that the present encryption strength in use for transmitting outbound data is less than said appropriate encryption strength, then in said controlling step an encryption strength appropriate for transmission of said outbound data is negotiated before transmission.

141. The method of claim 138 wherein if in said analysing step it is determined that the present encryption strength in use for transmitting outbound data is less than said appropriate encryption strength, then in said controlling step the outbound data is modified such that the present encryption strength is an appropriate encryption strength.

142. The method of claim 138 wherein in said analysing step if it is determined that the present encryption strength in use for transmitting outbound data is less than said appropriate encryption strength, then in said controlling step a user of said application is notified that the encryption strength in use is not sufficient.

143. The method of claim 136 wherein said analysing step includes identifying credit card numbers in said outbound data.

144. The method of claim 143 wherein said analysing step includes distinguishing a pre-determined set of one or more credit card numbers from other credit card numbers, and wherein said rules of said policy data define a different appropriate encryption strength for outbound data containing credit card numbers in that pre-determined set than for other credit card numbers.

145. The method of claim 144 wherein said rules of said policy data specifies that there is no appropriate encryption strength for said pre-determined set of one or more credit card numbers.

146. The method of claim 136 wherein said analysing step includes identifying at least one or more of, credit card numbers, account codes, usernames, passwords, names and addresses and other predetermined keywords in the content of said outbound data.

147. The method of claim 136 wherein said rules in said policy data specify an appropriate encryption strength for said outbound data, that is dependent on the address to which said outbound data is to be transmitted.

148. The method of claim 136 wherein said analysing step is performed at said one or more workstations.

149. The method of claim 136 wherein said application is a web browser.

150. The method of claim 149 wherein said analysing step is performed by a plug-in module of said web browser.

151. The method of claim 150 wherein said web browser is Microsoft's Internet Explorer and said plug-in module is a Browser Helper Object.

152. The method of claim 136 wherein said application is an e-mail client.

153. The method of claim 152 wherein said analysing step is performed by a plug-in module of said e-mail client.

154. The method of claim 153 wherein said e-mail client is Microsoft's Outlook e-mail client and said plug-in module is a Microsoft Exchange client extension.

155. The method of claim 136 wherein said network comprises a server and said analysing step is performed at a point on said network intermediate said one or more workstations and said server, or said analysing step is performed at said server.

156. The method of claim 136 wherein said computer network to which said one or more workstations are adapted for connection is a public computer network, and wherein said one or more workstations together form a private computer network.

157. The method of claim 136 further comprising the step of providing a supervisor workstation, said policy data being accessible by said supervisor workstation, such that a user of said supervisor workstation can edit said policy data.

158. A computer program product for controlling a computer connected to a public network to manage information, the computer having access to policy data containing rules specifying an appropriate encryption strength for outbound data transmitted to the public network, the encryption strength depending on the content of the data, comprising:

a recording medium readable by the computer, having program code recorded thereon which when executed on said computer, configures said computer to:

determine, in conjunction with an application running on the computer that is operable at least to transmit outbound data to said public network, with reference to said rules in said policy data, an

appropriate encryption strength for the outbound data; and

control the transmission of said outbound data by said application in dependence upon the determination of an appropriate encryption strength.

159. The computer program product of claim 158 wherein said rules in said policy data define confidential data which cannot be transmitted, wherein said program code when executed on said computer is operable to prevent transmission of said confidential data from said application.

160. The computer program product of claim 158 wherein said program code when executed on said computer is further operable to determine the present encryption strength in use for transmitting said outbound data; and

to control the transmission of said outbound data from said application in dependence upon both the determination of an appropriate encryption strength and the determination of the present encryption strength in use.

161. The computer program product of claim 160 wherein said program code when executed on said computer is further operable, if it is determined that the present encryption strength in use for transmitting outbound data is less than said appropriate encryption strength, to prevent the transmission of said outbound data from said application.

162. The computer program product of claim 160 wherein said program code when executed on said computer is further operable, if it is determined that the present encryption strength in use for transmitting outbound data is less than said appropriate encryption strength, to negotiate an appropriate encryption

strength for transmission of said outbound data before transmission.

163. The computer program product of claim 160 wherein said program code when executed on said computer is further operable, if it is determined that the present encryption strength in use for transmitting outbound data is less than said appropriate encryption strength, to modify the outbound data such that the present encryption strength is an appropriate encryption strength.

164. The computer program product of claim 160 wherein said program code when executed on said computer is further operable, if it is determined that the present encryption strength in use for transmitting outbound data is less than said appropriate encryption strength, to provide notification that the encryption strength in use is not sufficient.

165. The computer program product of claim 158 wherein said program code when executed on said computer is further operable to identify credit card numbers in said outbound data.

166. The computer program product of claim 165 wherein said program code when executed on said computer is further operable to identify a pre-determined set of one or more credit card numbers from other credit card numbers, and wherein said rules of said policy data define a different appropriate encryption strength for outbound data containing credit card numbers in that pre-determined set than for other credit card numbers.

167. The computer program product of claim 166 wherein said rules of said policy data specifies that

there is no appropriate encryption strength for said pre-determined set of one or more credit card numbers.

168. The computer program product of claim 158 wherein said program code when executed on said computer is further operable, to identify at least one or more of, credit card numbers, account codes, usernames, passwords, names and addresses and other predetermined keywords in the content of said outbound data.

169. The computer program product of claim 158 wherein said rules in said policy data specify an appropriate encryption strength for said outbound data, that is dependent on the address to which said outbound data is to be transmitted.

170. The computer program product of claim 158 wherein said program code is executable on said computer.

171. The computer program product of claim 158 wherein said application is a web browser.

172. The computer program product of claim 171 wherein said program code when executed on said computer is a plug-in module of said web browser.

173. The computer program product of claim 172 wherein said web browser is Microsoft's Internet Explorer and said plug-in module is a Browser Helper Object.

174. The computer program product of claim 158 wherein said application is an e-mail client.

175. The computer program product of claim 174 wherein said program code when executed on said computer is a plug-in module of said e-mail client.

176. The computer program product of claim 175 wherein said e-mail client is Microsoft's Outlook e-mail client and said plug-in module is a Microsoft Exchange client extension.

177. The computer program product of claim 158 wherein said network includes a server and said program code is executable at a point on said network intermediate said one or more workstations and said server, or program code is executable at said server.

178. An information management system comprising:

a plurality of client workstations adapted for connection to a computer network, each workstation having a memory;

a data repository arranged to receive data from each of said client workstations;

an application stored in said memory of each workstation for transmitting outbound data to said network and receiving inbound data from said network;

policy data defining rules for the recording of data that may comprise part of a transaction conducted between a client workstation and a third party across said computer network;

an analyser, said analyser being operable in conjunction with said policy data to analyse at least one of said outbound data and said inbound data, to identify the existence of a transaction occurring between a client workstation and a third party by analysing said outbound or said inbound data, and to cause transaction data that is all or part of said outbound data or said inbound data related to an

identified transaction to be stored in said data repository.

179. The system of claim 178 wherein said analyser is operable to determine whether a secure link has been negotiated between said application and a remote site on said network, and to identify the existence of a transaction if said outbound data or said inbound data is transmitted on a secure link.

180. The system of claim 179 wherein said network is the Internet, and said rules of said policy data define the addresses of non-eCommerce web sites and/or non-eCommerce e-mail accounts, said analyser being operable to disregard any transactions that are identified between a client workstation and a non-eCommerce web site and/or e-mail account such that no transaction data related to a transaction made to a non-eCommerce web sites or a non-eCommerce e-mail account is stored in the data repository.

181. The system of claim 178 wherein said analyser is operable to identify the existence of a transaction by reference to said rules of said policy data, said rules of said policy data defining the addresses of known eCommerce locations.

182. The system of claim 178 wherein said analyser is operable to identify credit card numbers, and to identify the existence of a transaction by identifying credit card numbers in said outbound data or inbound data.

183. The system of claim 178 wherein said analyser is operable to identify the existence of a transaction by reference to said rules of said policy data, said rules of said policy data defining one or more of pre-determined digital certificates, account codes, pre-

determined keywords, pre-determined names and addresses and embedded codes.

184. The system of claim 178 wherein said analyser is operable to identify embedded codes in said inbound data, said embedded code having been placed in said inbound data to identify it as transaction data.

185. The system of claim 178 wherein said analyser is operable to identify electronic receipts, and to identify the existence of a transaction by identifying an electronic receipt in said outbound or inbound data.

186. The system of claim 178 wherein said analyser is operable to record a pre-determined number of subsequent transmissions of said outbound data or said inbound data following an identification of the existence of a transaction by said analyser, providing that the address or organisation to which the subsequent transmissions are sent, or from which they are received, is the same as the address or organisation to which the outbound data was sent or from which the inbound data was received and in which the existence of a transaction was identified.

187. The system of claim 186, wherein said analyser is operable to detect one or more indicators of the nature of the transaction, and said rules of said policy data define the number of subsequent transmissions of said outbound data and said inbound data that are to be recorded in said data repository based on the identified nature of the transaction.

188. The system of claim 186 wherein said rules of said policy data define the number of subsequent transmissions of said outbound and said inbound data that are to be stored in said data repository in

dependence on the indicator by which the existence of a transaction was identified.

189. The system of claim 178 wherein said analyser is operable to record all subsequent transmissions of said outbound data or said inbound data that occur within a pre-determined amount of time following an identification of the existence of a transaction by said analyser, providing that the address or organisation to which the subsequent transmissions are sent, or from which they are received, is the same as the address or organisation to which the outbound data was sent or from which the inbound data was received and in which the existence of a transaction was identified.

190. The system of claim 189, wherein said analyser is operable to detect one or more indicators of the nature of the transaction, and said rules of said policy data define the amount of time for which all subsequent transmissions of said outbound data and said inbound data are to be recorded in said data repository based on the identified nature of the transaction.

191. The system of claim 189 wherein said rules of said policy data define the amount of time for which subsequent transmissions of said outbound and said inbound data are to be stored in said data repository in dependence on the indicator by which the existence of a transaction was identified.

192. The system of claim 178 wherein said analyser is further operable to identify the completion of a transaction by analysing said outbound data or said inbound data, and to cause all or part of said outbound data transmitted by said application and all or part of said inbound data received by said application after

said analyser has identified the existence of a transaction and before said analyser has identified the completion of a transaction to be stored in said data repository.

193. The system of claim 192 wherein said analyser is operable to identify subsequent related data in said outbound data transmitted by said application and said inbound data received by said application after said analyser has identified the completion of a transaction, and to cause said subsequent related data to be stored in said data repository with said transaction data already identified.

194. The system of claim 193 wherein said analyser is operable to identify said subsequent related data by identifying common indicators in both said transaction data already identified and said outbound data transmitted by said application and said inbound data received by said application after said analyser has identified the completion of a transaction, said common indicators being one or more of the address of the location to which said outbound data is transmitted or from which said inbound data is received, part of the data path to the location to which said outbound data is transmitted or from which said inbound data is received, account code or reference numbers.

195. The system of claim 178 wherein said application is operable such that a user of said application can indicate said outbound and said inbound data that is related to a transaction, said analyser being operable to identify said outbound and said inbound data so indicated.

196. The system of claim 178 wherein said application is operable to store all of said outbound data and said inbound data in said memory of said

workstation as previous data, irrespective of whether it may or may not be part of a transaction and, said analyser is operable, if the existence of a transaction is identified, to retrieve a pre-determined amount of previous data from said outbound data and said inbound data stored in said memory of said workstation, and to cause said previous data to be stored in said data repository with said transaction data.

197. The system of claim 196 wherein said rules of said policy data specify the amount of previous data that is to be retrieved in dependence on the indicator by which the existence of a transaction is identified.

198. The system of claim 196 wherein said network is the Internet and said application is a web browser, said web browser being operable to store each web page that is viewed by said web browser in memory as previous data.

199. The system of claim 198 wherein said rules of said policy data specify the number of web pages that are to be retrieved from those previously stored in memory in dependence on the indicator by which the existence of a transaction is identified.

200. The system of claim 178 wherein said application is operable to store all of said outbound data and said inbound data in memory as previous data, irrespective of whether it may or may not be part of a transaction and, said analyser is operable, if the existence of a transaction is identified, to identify, in said previous data, earlier relevant data that is related to said transaction data already identified, and to cause said earlier relevant data to be stored in said data repository with said transaction data.

201. The system of claim 200 wherein said analyser is operable to identify said earlier relevant data in said previous data, by identifying common indicators in both said transaction data and said outbound data and said inbound data previously stored in said memory of said workstation, said common indicators being one or more of the address of the location to which said outbound data is transmitted or from which said inbound data is received, part of the data path to the location to which said outbound data is transmitted or said inbound data is received, account code or reference number.

202. The system of claim 178 wherein said application is operable to store all of said outbound data and said inbound data in memory as previous data, irrespective of whether it may or may not be part of a transaction, and is further operable such that, if said analyser identifies the existence of a transaction, a user of said application can select earlier relevant data from said previous data, said earlier relevant data selected by the user being stored in said common data repository together with said transaction data.

203. The system of claim 178 wherein said analyser is operable, once it has identified the existence of a transaction, to determine the nature of said transaction by analysing the content of said outbound and inbound data, and said rules of said policy data define how said transaction data is to be stored in said data repository in dependence on the nature of the transaction determined by said analyser, said transaction data being stored in said database according to said determination and said rules of said policy data.

204. The system of claim 203 wherein said analyser is operable to determine the nature of the transaction

by identifying in said outbound data and said inbound data one or more indicators, said indicators being defined in said rules of said policy data, and being one or more of: the address of the network location to which said data that may be part of a transaction is transmitted or from which it is received; part of the data path to the network location to which said transaction data is transmitted or from which it is received; account codes; reference numbers; credit card numbers; digital certificates and pre-determined keywords.

205. The system of claim 178 wherein said analyser is operable to identify, once the existence of a transaction has been identified, one or more indicators of the nature of said transaction, said transaction data being stored in said data repository such that it is organised by said one or more indicators to form a record.

206. The system of claim 205 wherein said rules of said policy data define said one or more indicators of the nature of a transaction, said indicators being one or more of: the address of the location to which said transaction data is transmitted or from which it is received; part of the data path to the location to which said transaction data is transmitted or from which it is received; account codes, reference numbers, credit card numbers, digital certificates and pre-determined keywords.

207. The system of claim 178 wherein said data repository is accessible by one or more of an accounts application, an order processing application or other transaction management application.

208. The system of claim 178 wherein any data transmitted to said data repository is encrypted before it is transmitted to said data repository.

209. The system of claim 178 wherein any data stored in said data repository is encrypted.

210. The system of claim 178 wherein said analyser is located on each of said one or more workstations.

211. The system of claim 178 wherein said application is a web browser.

212. The system of claim 211 wherein said analyser is a plug-in module of said web browser.

213. The system of claim 212 wherein said web browser is Microsoft's Internet Explorer and said analyser is a Browser Helper Object.

214. The system of claim 178 wherein said application is an e-mail client.

215. The system of claim 214 wherein said analyser is a plug-in module of said e-mail client.

216. The system of claim 215 wherein said e-mail client is Microsoft's Outlook e-mail client and said analyser is a Microsoft Exchange client extension.

217. The system of claim 178 wherein said network comprises a server, and said analyser is located at a point on said network intermediate said one or more work stations and said server, or said analyser is located at said server.

218. The system of claim 178 wherein said computer network to which said one or more workstations are

adapted for connection is a public computer network, and wherein said one or more workstations together form a private computer network.

219. The system of claim 178 further comprising a supervisor workstation, said policy data being accessible by said supervisor workstation, such that a user of said supervisor workstation can edit said policy data.

220. A method of managing information comprising the steps of:

providing a plurality of client workstations adapted for connection to a computer network, each workstation having a memory;

providing a data repository arranged to receive data from each of said client workstations;

providing an application stored in said memory of each workstation for transmitting outbound data to said network and receiving inbound data from said network;

providing policy data defining rules for the recording of data that may comprise part of a transaction conducted between a client workstation and a third party across said computer network; and

analysing, at least one of said outbound data and said inbound data to identify, with reference to said rules of said policy data, the existence of a transaction occurring between a client workstation and a third party; and

storing transaction data that is all or part of said outbound data or said inbound data related to an identified transaction in said data repository.

221. The method of claim 220 wherein in said analysing step the existence of a transaction is identified by determining whether a secure link has been negotiated between said application and a remote

site on said network, and by determining whether said outbound data or said inbound data is transmitted on that link.

222. The method of claim 221 wherein said network is the Internet, and said rules of said policy data define the addresses of non-eCommerce web sites and/or non-eCommerce e-mail accounts, wherein said analysing step includes disregarding any transactions that are identified between a client workstation and a non-eCommerce web site and/or e-mail account such that no transaction data related to a transaction made to a non-eCommerce web site or a non-eCommerce e-mail account is stored in the data repository.

223. The method of claim 220 wherein said analysing step includes identifying the existence of a transaction by reference to said rules of said policy data, said rules of said policy data defining the addresses of known eCommerce locations.

224. The method of claim 220 wherein said analysing step includes identifying credit card numbers, and the existence of a transaction is identified by identifying credit card numbers in said outbound data or inbound data.

225. The method of claim 220 wherein in said analysing step the existence of a transaction is identified by reference to said rules of said policy data, said rules of said policy data defining one or more of pre-determined digital certificates, account codes, pre-determined keywords, pre-determined names and addresses and embedded codes.

226. The method of claim 220 wherein said analysing step includes detecting an embedded code in said inbound data, said embedded code having been

placed in said inbound data to identify it as transaction data.

227. The method of claim 220 wherein in said analysing step, the existence of a transaction is identified by identifying an electronic receipt in said outbound or inbound data.

228. The method of claim 220 further comprising the step of recording a pre-determined number of subsequent transmissions of said outbound data or said inbound data following an identification of the existence of a transaction in said analysing step, providing that the address or organisation to which the subsequent transmissions are sent, or from which they are received, is the same as the address or organisation to which the outbound data was sent or from which the inbound data was received and in which the existence of a transaction was identified.

229. The method of claim 228, wherein said analysing step includes detecting one or more indicators of the nature of the transaction, and said rules of said policy data define the number of subsequent transmissions of said outbound data and said inbound data that are to be recorded in said data repository based on the identified nature of the transaction.

230. The method of claim 228 wherein said rules of said policy data define the number of subsequent transmissions of said outbound and said inbound data that are to be stored in said data repository in dependence on the indicator by which the existence of a transaction was identified.

231. The method of claim 220 further comprising the step of recording all subsequent transmissions of

said outbound data or said inbound data that occur within a pre-determined amount of time following an identification of the existence of a transaction in said analysing step, providing that the address or organisation to which the subsequent transmissions are sent, or from which they are received, is the same as the address or organisation to which the outbound data was sent or from which the inbound data was received and in which the existence of a transaction was identified.

232. The method of claim 231, wherein said analysing step includes detecting one or more indicators of the nature of the transaction, and said rules of said policy data define the amount of time for which all subsequent transmissions of said outbound data and said inbound data are to be recorded in said data repository based on the identified nature of the transaction.

233. The method of claim 231 wherein said rules of said policy data define the amount of time for which subsequent transmissions of said outbound and said inbound data are to be stored in said data repository in dependence on the indicator by which the existence of a transaction was identified.

234. The method of claim 220 wherein said analysing step includes identifying the completion of a transaction by analysing said outbound data or said inbound data, and said storing step includes storing all or part of said outbound data transmitted by said application and all or part of said inbound data received by said application, after the existence of a transaction has been identified and before the completion of a transaction has been identified, in said data repository.

235. The method of claim 234 wherein said analysing step includes identifying subsequent related data contained in said outbound data transmitted by said application and said inbound data received by said application after the completion of a transaction, and said storing step includes storing said subsequent related data in said data repository with said transaction data already identified.

236. The method of claim 235 wherein said analysing step includes identifying said subsequent related data by identifying common indicators in both said transaction data already identified and said outbound data transmitted by said application and said inbound data received by said application after the completion of a transaction has been identified, said common indicators being one or more of the address of the location to which said outbound data is transmitted or from which said inbound data is received, part of the data path to the location to which said outbound data is transmitted or from which said inbound data is received, account code or reference numbers.

237. The method of claim 220 wherein said application is operable such that a user of said application can indicate said outbound and said inbound data that is related to a transaction, said analysing step including identifying indicated outbound and inbound data.

238. The method of claim 220 further comprising the step of storing all of said outbound data and said inbound data in said memory of said workstation as previous data, irrespective of whether it may or may not be part of a transaction and, said analysing step includes retrieving a pre-determined amount of previous data from said outbound data and said inbound data

stored in said memory of said workstation if the existence of a transaction is identified, and said storing step includes storing said previous data in said data repository with said transaction data.

239. The method of claim 238 wherein said rules of said policy data specify the amount of previous data that is to be retrieved in dependence on the indicator by which the existence of a transaction is identified.

240. The method of claim 238 wherein said network is the Internet and said application is a web browser, said web browser being operable to store each web page that is viewed by said web browser in memory as previous data.

241. The method of claim 240 wherein said rules of said policy data specify the number of web pages that are to be retrieved from those previously stored in memory in dependence on the indicator by which the existence of a transaction is identified.

242. The method of claim 220 further comprising the step of storing all of said outbound data and said inbound data in memory as previous data, irrespective of whether it may or may not be part of a transaction and, said analysing step includes identifying, in said previous data, earlier relevant data that is related to said transaction data already identified, and said storing step includes storing said earlier relevant data in said data repository with said transaction data.

243. The method of claim 242 wherein said analysing step includes identifying said earlier relevant data in said previous data, by identifying common indicators in both said transaction data and

said previous data, said common indicators being one or more of the address of the location to which said outbound data is transmitted or from which said inbound data is received, part of the data path to the location to which said outbound data is transmitted or said inbound data is received, account code or reference number.

244. The method of claim 220 further comprising the steps of storing all of said outbound data and said inbound data in memory as previous data, irrespective of whether it may or may not be part of a transaction; and

if the existence of a transaction is identified, providing a user of said application with a selector for selecting earlier relevant data from said previous data, and wherein said storing step includes storing said earlier relevant data selected by the user in said data repository together with said transaction data.

245. The method of claim 220 wherein said analysing step includes, once the existence of a transaction has been identified, determining the nature of said transaction by analysing the content of said outbound and inbound data, said rules of said policy data defining how said transaction data is to be stored in said data repository in dependence on the nature of the transaction determined in said analysing step, said transaction data being stored in said database according to said determination and said rules of said policy data.

246. The method of 245 wherein said analysing step includes determining the nature of the transaction by identifying in said outbound data and said inbound data one or more indicators, said indicators being defined in said rules of said policy data, and being one or

more of: the address of the network location to which said data that may be part of a transaction is transmitted or from which it is received; part of the data path to the network location to which said transaction data is transmitted or from which it is received; account codes; reference numbers; credit card numbers; digital certificates and pre-determined keywords.

247. The method of claim 220 wherein said analysing step includes identifying, once the existence of a transaction has been identified, one or more indicators of the nature of said transaction, and said storing step includes organising transaction data stored in said data repository by said one or more indicators such that it forms a record.

248. The method of claim 247 wherein said rules of said policy data define said one or more indicators of the nature of a transaction, said indicators being one or more of: the address of the location to which said transaction data is transmitted or from which it is received; part of the data path to the location to which said transaction data is transmitted or from which it is received; account codes, reference numbers, credit card numbers, digital certificates and pre-determined keywords.

249. The method of claim 220 wherein said data repository is accessible by one or more of an accounts application, an order processing application or other transaction management application.

250. The method of claim 220 further comprising the step of encrypting any relevant data identified in said analysing step before it is stored in said data repository.

251. The method of claim 220 further comprising the step of encrypting the data stored in said data repository.

252. The method of claim 220 wherein said analysing step is performed at said one or more workstations.

253. The method of claim 220 wherein said application is a web browser.

254. The method of claim 253 wherein said analysing step is performed by a plug-in module of said web browser.

255. The method of claim 254 wherein said web browser is Microsoft's Internet Explorer and said plug-in module is a Browser Helper Object.

256. The method of claim 220 wherein said application is an e-mail client.

257. The method of claim 256 wherein said analysing step is performed by a plug-in module of said e-mail client.

258. The method of claim 257 wherein said e-mail client is Microsoft's Outlook e-mail client and said plug-in module is a Microsoft Exchange client extension.

259. The method of claim 220 wherein said network comprises a server, and said analysing step is performed at a point on said network intermediate said one or more work stations and said server, or said analysing step is performed at said server.

260. The method of claim 220 wherein said computer network to which said one or more workstations are adapted for connection is a public computer network, and wherein said one or more workstations together form a private computer network.

261. The method of claim 220 further comprising the step of providing a supervisor workstation, said policy data being accessible by said supervisor workstation, such that a user of said supervisor workstation can edit said policy data.

262. A computer program product for controlling a plurality of computers in a private network to manage information, the network having a data repository arranged to receive data from the plurality of computers, and policy data defining rules for the recording of data that may comprise part of a transaction conducted between a computer in the private network and a third party across a public network, comprising:

a recording medium readable by a computer, having program code recorded thereon which when executed on each of said plurality of computers configures said computers to:

analyse, in conjunction with an application running on the computer that is operable to transmit outbound data to said public network and receive inbound data from said public network, at least one of said outbound data and said inbound data to identify, with reference to said rules of said policy data, the existence of a transaction occurring between the computer and a third party; and

to control said computer to store transaction data that is all or part of said outbound data or said inbound data related to an identified transaction in said data repository.

263. The computer program product of claim 262 wherein said program code when executed on said computer is operable to identify the existence of a transaction by determining whether a secure link has been negotiated between said application and a remote site on said public network, and whether the outbound data or said inbound data is transmitted on that link.

264. The computer program product of claim 263 wherein said public network is the Internet, and said rules of said policy data define the addresses of non-eCommerce web sites and/or non-eCommerce e-mail accounts, wherein said program code when executed on said computer is operable to disregard any transactions that are identified between the computer and a non-eCommerce web site and/or e-mail account such that no transaction data related to a transaction made to a non-eCommerce web sites or a non-eCommerce e-mail account is stored in the data repository.

265. The computer program product of claim 262 wherein said program code when executed on said computer is operable to identify the existence of a transaction by reference to said rules of said policy data, said rules of said policy data defining the addresses of known eCommerce locations.

266. The computer program product of claim 262 wherein said program code when executed on said computer is operable to identify credit card numbers, and the existence of a transaction is identified by identifying credit card numbers in said outbound data or inbound data.

267. The computer program product of claim 262 wherein said program code when executed on said computer is operable to identify the existence of a transaction by reference to said rules of said policy

data, said rules of said policy data defining one or more of pre-determined digital certificates, account codes, pre-determined keywords, pre-determined names and addresses and embedded codes.

268. The computer program product of claim 262 wherein said program code when executed on said computer is operable to identify in said inbound data an embedded code, said embedded code having been placed in said inbound data to identify it as transaction data.

269. The computer program product of claim 262 wherein said program code when executed on said computer is operable to identify the existence of a transaction by identifying an electronic receipt in said outbound or inbound data.

270. The computer program product of claim 262 wherein said program code when executed on said computer is further operable to control the computer to record a pre-determined number of subsequent transmissions of said outbound data or said inbound data following an identification of the existence of a transaction, providing that the address or organisation to which the subsequent transmissions are transmitted, or from which they are received, is the same as the address or organisation to which the outbound data was sent or from which the inbound data was received and in which the existence of a transaction was identified.

271. The computer program product of claim 270, wherein said program code when executed on said computer is operable to detect one or more indicators of the nature of the transaction, and said rules of said policy data define the number of subsequent transmissions of said outbound data and said inbound

data that are to be recorded in the data repository based on the identified nature of the transaction.

272. The computer program product of claim 270 wherein said rules of said policy data define the number of subsequent transmissions of said outbound and said inbound data that are to be stored in said data repository in dependence on the indicator by which the existence of a transaction was identified.

273. The computer program product of claim 262 wherein said program code when executed on said computer is operable to control the computer to record all subsequent transmissions of said outbound data or said inbound data that occur within a pre-determined amount of time following an identification of the existence of a transaction, providing that the address or organisation to which the subsequent transmissions are transmitted, or from which they are received, is the same as the address or organisation to which the outbound data was transmitted or from which the inbound data was received and in which the existence of a transaction was identified.

274. The computer program product of claim 273 wherein said program code when executed on said computer is operable to detect one or more indicators of the nature of the transaction, and said rules of said policy data define the amount of time for which all subsequent transmissions of said outbound data and said inbound data are to be recorded in said data repository based on the identified nature of the transaction.

275. The computer program product of claim 273 wherein said rules of said policy data define the amount of time for which subsequent transmissions of said outbound and said inbound data are to be stored in

said data repository in dependence on the indicator by which the existence of a transaction was identified.

276. The computer program product of claim 262 wherein said program code when executed on said computer is operable to identify the completion of a transaction, and control the computer to store all or part of said outbound data transmitted by said application and all or part of said inbound data received by said application after the existence of a transaction has been identified and before the completion of a transaction has been in identified in said data repository.

277. The computer program product of claim 276 wherein said program code when executed on said computer is operable to identify subsequent related data contained in said outbound data transmitted by said application and said inbound data received by said application after the completion of a transaction, and control the computer to store said subsequent related data in the data repository with said transaction data already identified.

278. The computer program product of claim 277 wherein said program code when executed on said computer is operable to identify said subsequent related data by identifying common indicators in both said transaction data already identified and said outbound data transmitted by said application and said inbound data received by said application after the completion of a transaction has been identified,

said common indicators being one or more of the address of the location to which said outbound data is transmitted or from which said inbound data is received, part of the data path to the location to which said outbound data is transmitted or from which

said inbound data is received, account code or reference numbers.

279. The computer program product of claim 262 wherein said application is operable such that a user of said application can indicate said outbound and said inbound data that is related to a transaction, said program code when executed on said computer being operable to identify said outbound and said inbound data so indicated.

280. The computer program product of claim 262 wherein said program code when executed on said computer is operable to control the computer to store all of said outbound data and said inbound data in memory as previous data, irrespective of whether it may or may not be part of a transaction and, to retrieve a pre-determined amount of previous data from said outbound data and said inbound data stored in memory if the existence of a transaction is identified, and to control the computer to store said previous data in the data repository with said transaction data.

281. The computer program product of claim 280 wherein said rules of said policy data specify the amount of previous data that is to be retrieved in dependence on the indicator by which the existence of a transaction is identified.

282. The computer program product of claim 280 wherein said public network is the Internet and said application is a web browser, said web browser being operable to store each web page that is viewed by said web browser in memory as previous data.

283. The computer program product of claim 282 wherein said rules of said policy data specify the number of web pages that are to be retrieved from those

previously stored in memory in dependence on the indicator by which the existence of a transaction is identified.

284. The computer program product of claim 262 wherein said program code when executed on said computer is further operable to control the computer to store all of said outbound data and said inbound data in memory as previous data, irrespective of whether it may or may not be part of a transaction and, to identify, in said previous data, earlier relevant data that is related to said transaction data already identified, and control the computer to store the earlier relevant data in the data repository with said transaction data.

285. The computer program product of claim 284 wherein said program code when executed on said computer is further operable to identify said earlier relevant data in said previous data, by identifying common indicators in both said transaction data and said previous data, said common indicators being one or more of the address of the location to which said outbound data is transmitted or from which said inbound data is received, part of the data path to the location to which said outbound data is transmitted or said inbound data is received, account codes or reference numbers.

286. The computer program product of claim 262 wherein said program code when executed on said computer is further operable to control the computer to store all of said outbound data and said inbound data in memory as previous data, irrespective of whether it may or may not be part of a transaction; and

wherein said computer program product further comprises a selector, recorded on said recording medium, said selector being operable to

select earlier relevant data from said previous data in response to input from a user,

and wherein said program code when executed on said computer is further operable to control the computer to store said earlier relevant data selected by the user in said data repository together with said transaction data.

287. The computer program product of claim 262 wherein said program code when executed on said computer is operable, once the existence of a transaction has been identified, to determine the nature of said transaction by analysing the content of said outbound and inbound data,

said rules of said policy data defining how said transaction data is to be stored in said data repository in dependence on the nature of the transaction that has been determined, said transaction data being stored in said database according to said determination and said rules of said policy data.

288. The computer program product of claim 287 wherein said program code when executed on said computer is further operable to determine the nature of the transaction by identifying in said outbound data and said inbound data one or more indicators, said indicators being defined in said rules of said policy data, and being one or more of: the address of the public network location to which said data that may be part of a transaction is transmitted or from which it is received; part of the data path to the public network location to which said transaction data is transmitted or from which it is received; account codes; reference numbers; credit card numbers; digital certificates and pre-determined keywords.

289. The computer program product of claim 262 wherein said program code when executed on said

computer is further operable, once the existence of a transaction has been identified, to identify one or more indicators of the nature of said transaction, and to control the computer to organise the storage of said transaction data by said one or more indicators such that it forms a record.

290. The computer program product of claim 289 wherein said rules of said policy data define said one or more indicators of the nature of a transaction, said indicators being one or more of: the address of the public location to which said transaction data is transmitted or from which it is received; part of the data path to the public location to which said transaction data is transmitted or from which it is received; account codes, reference numbers, credit card numbers, digital certificates and pre-determined keywords.

291. The computer program product of claim 262 wherein the data repository is accessible by one or more of an accounts application, an order processing application or other transaction management application.

292. The computer program product of claim 262 wherein said program code when executed on said computer is further operable to cause any identified relevant data to be encrypted before it is stored in said data repository.

293. The computer program product of claim 262 wherein said program code when executed on said computer is further operable to cause any relevant data stored in the data repository to be encrypted.

294. The computer program product of claim 262 wherein said program code is executable at each of said computers.

295. The computer program product of claim 262 wherein said application is a web browser.

296. The computer program product of claim 295 wherein said program code when executed on said computer is a plug-in module of said web browser.

297. The computer program product of claim 296 wherein said web browser is Microsoft's Internet Explorer and said plug-in module is a Browser Helper Object.

298. The computer program product of claim 262 wherein said application is an e-mail client.

299. The computer program product of claim 298 wherein said program code when executed on said computer is a plug-in module of said e-mail client.

300. The computer program product of claim 299 wherein said e-mail client is Microsoft's Outlook e-mail client and said plug-in module is a Microsoft Exchange client extension.

301. Computer program product of claim 262 wherein said network includes a server and said program code is executable at a point on said network intermediate said one or more workstations and said server, or said program code is executable at said server.

302. The computer program product of claim 262 further comprising program code recorded on the recording medium which when executed on a computer in the plurality of computers enable that computer as a

supervisor workstation, said supervisor workstation having access to said data repository and being operable to view said relevant data stored in said data repository.

303. The computer program product of claim 302 wherein said policy data is accessible by said supervisor workstation, such that a user of said supervisor workstation can edit said policy data.

304. An information management system comprising:

one or more workstations adapted for connection to a computer network, each workstation having a memory;

an application stored in said memory of each workstation for transmitting outbound data to said network and receiving inbound data from said network;

policy data, containing rules for the transmission of outbound data that may be part of a transaction; and

an analyser, said analyser being operable in conjunction with said policy data to identify in at least said outbound data, transaction data that may be part of a transaction, and to make a determination in accordance with said rules of said policy data as to whether the transmission of said transaction data would satisfy said rules;

and wherein the transmission of said transaction data by said application is dependent on said determination made by said analyser.

305. The system of claim 304, wherein according to said determination made by said analyser, said transaction data is either, transmitted, not transmitted, or sent to an approver who determines whether or not to transmit the transaction data.

306. The system of claim 305 further comprising:

one or more approvers, for deciding whether the transmission of said data that may be part of a transaction may be made;

wherein said analyser is operable to identify in said data that may be part of a transaction, data that needs approval and to refer said data that needs approval to one of said one or more approvers; and

the transmission of said data that needs approval being dependent on the decision of said one or more approver.

307. The system of claim 306 wherein said analyser is operable to identify said transaction data that needs approval by determining the nature of said transaction data and by checking said rules of said policy data, said rules of said policy data defining whether or not approval is needed in dependence on the determined nature of said transaction data.

308. The system of claim 306 wherein said analyser is operable to determine the nature of said transaction data by identifying at least one of the identity of the transmitter of said data, the identity of the intended recipient of said data, the workstation from which said data is to be transmitted, the sum for which a transaction is to be made, and the account against which a transaction is to be made.

309. The system of claim 306 wherein said analyser is operable to determine the nature of said transaction data that needs approval and to select said one of said one or more approvers in dependence on that determination.

310. The system of claim 309 wherein said analyser is operable to determine the nature of said transaction data that needs approval by identifying at least one of the identity of the transmitter of said data, the

identity of the intended recipient of said data, the work station from which said data is to be transmitted, the sum for which a transaction is to be made, and the account against which the transaction is to be made.

311. The system of claim 304 wherein said analyser is operable to determine whether a secure link has been negotiated between said application and a remote site on said network, and to identify said outbound data or said inbound data as transaction data, if it is transmitted on a secure link.

312. The system of claim 311 wherein said network is the Internet, and said rules of said policy data define the addresses of web sites or e-mail accounts that negotiate secure links for the transmission of data but which are known not to be eCommerce sites or accounts, said analyser being operable to disregard said outbound data transmitted to those web sites or accounts or said inbound data received from those web sites or accounts, such that no approval is required.

313. The system of claim 304 wherein said analyser is operable to identify transaction data by reference to said rules of said policy data, said rules of said policy data defining the addresses of known eCommerce web sites and e-mail accounts.

314. The system of claim 304 wherein said analyser is operable to identify credit card numbers in said outbound data or said inbound data, and to identify outbound data or inbound data that contains a credit card number as transaction data.

315. The system of claim 314 wherein said policy data specifies pre-determined credit card numbers that can never be transmitted.

316. The system of claim 304 wherein said analyser is operable to identify transaction data by reference to said rules of said policy data, said rules of said policy data defining one or more of pre-determined digital certificates, account codes, pre-determined keywords, pre-determined names and addresses and embedded codes.

317. The system of claim 304 wherein said analyser is operable to identify embedded codes in said inbound data, said embedded codes having been placed in said inbound data to mark said inbound data as transaction data.

318. The system of claim 304 wherein said application is operable such that a user of said application can indicate said outbound and said inbound data that is part of a transaction, said analyser being operable to identify said outbound and said inbound data so indicated.

319. The system of claim 304 wherein said analyser is located on each of said one or more workstations.

320. The system of claim 304 wherein said application is a web browser.

321. The system of claim 320 wherein said analyser is a plug-in module of said web browser.

322. The system of claim 321 wherein said web browser is Microsoft's Internet Explorer and said analyser is a Browser Helper Object.

323. The system of claim 304 wherein said application is an e-mail client.

324. The system of claim 323 wherein said analyser is a plug-in module of said e-mail client.

325. The system of claim 324 wherein said e-mail client is Microsoft's Outlook e-mail client and said analyser is a Microsoft Exchange client extension.

326. The system of claim 304 wherein said network comprises a server and said analyser is located at a point on said network intermediate said one or more workstations and said server, or said analyser is located at said server.

327. The system of claim 304 wherein said computer network to which said one or more workstations are adapted for connection is a public computer network, and wherein said one or more workstations together form a private computer network.

328. The system of claim 304 further comprising a supervisor workstation, said policy data being accessible by said supervisor workstation, such that a user of said supervisor workstation can edit said policy data.

329. A method for managing information comprising the steps of:

providing one or more workstations adapted for connection to a computer network, each workstation having a memory;

providing an application stored in said memory of each workstation for transmitting outbound data to said network and receiving inbound data from said network;

providing policy data, containing rules for the transmission of outbound data that may be part of a transaction; and

analysing at least said outbound data to identify, with reference to said rule of said policy data, transaction data that may be part of a transaction;

determining, in accordance with said rules of said policy data, whether the transmission of said transaction data would satisfy said rules;

controlling transmission of said transaction data by said application in dependence on the determination made in said determining step.

330. The method of claim 329, wherein said controlling step includes said transaction data being either, transmitted, not transmitted, or sent to an approver who determines whether or not to transmit the transaction data.

331. The method of claim 330 further comprising the steps of:

identifying in said data that may be part of a transaction, data that needs approval;

referring said data that need approval to one or more approvers for approval; and

monitoring whether or nor approval is received from said one or more approvers;

and wherein in said controlling step, the transmission of said transaction data depends on whether or not approval is received from said one or more approvers.

332. The method of claim 331 wherein said analysing step includes identifying said transaction data that needs approval by determining the nature of said transaction data and checking said rules of said policy data, said rules of said policy data defining whether or not approval is needed in dependence on the determined nature of said transaction data.

333. The method of claim 331 wherein said analysing step includes determining the nature of said transaction data by identifying at least one of the identity of the transmitter of said data, the identity of the intended recipient of said data, the workstation from which said data is to be transmitted, the sum for which a transaction is to be made, and the account from which a transaction is to be made.

334. The method of claim 331 wherein said analysing step includes determining the nature of said transaction data that needs approval and selecting said one of said one or more approvers in dependence on that determination.

335. The method of claim 334 wherein said analysing step includes determining the nature of said transaction data that needs approval by identifying at least one of the identity of the transmitter of said data, the identity of the intended recipient of said data, the work station from which said data is to be transmitted, the sum for which a transaction is to be made, and the account from which the transaction is to be made.

336. The method of claim 329 wherein said analysing step includes determining whether a secure link has been negotiated between said application and a remote site on said network, and identifying said outbound data or said inbound data as transaction data, if it is transmitted on a secure link.

337. The method of claim 336 wherein said network is the Internet, and said rules of said policy data define the addresses of web sites or e-mail accounts that negotiate secure links for the transmission of data but which are known not to be eCommerce sites or accounts, and said analysing step includes disregarding

said outbound data transmitted to those web sites or accounts or said inbound data received from those web sites or accounts, such that no approval is required.

338. The method of claim 329 wherein said analysing step includes identifying transaction data by reference to said rules of said policy data, said rules of said policy data defining the addresses of known eCommerce web sites and e-mail accounts.

339. The method of claim 329 wherein said analysing step includes identifying credit card numbers in said outbound data or said inbound data, and identifying outbound data or inbound data that contains a credit card number as transaction data.

340. The method of claim 339 wherein said policy data specifies pre-determined credit card numbers that can never be transmitted.

341. The method of claim 329 wherein said analysing step includes identifying transaction data by reference to said rules of said policy data, said rules of said policy data defining one or more of pre-determined digital certificates, account codes, pre-determined keywords, pre-determined names and addresses and embedded codes.

342. The method of claim 329 wherein said analysing step includes detecting an embedded code in said inbound data, said embedded code having been placed in said inbound data to mark said inbound data as transaction data.

343. The method of claim 329 further comprising the step of providing a user of said application with a selector to indicate said outbound and said inbound data that is part of a transaction, said analysing step

including identifying selected outbound and inbound data.

344. The method of claim 329 wherein said analysing step is performed at said one or more workstations.

345. The method of claim 329 wherein said application is a web browser.

346. The method of claim 345 wherein said analysing step is a plug-in module of said web browser.

347. The method of claim 346 wherein said web browser is Microsoft's Internet Explorer and said plug0in module is a Browser Helper Object.

348. The method of claim 329 wherein said application is an e-mail client.

349. The method of claim 348 wherein said analysing step is performed by a plug-in module of said e-mail client.

350. The method of claim 349 wherein said e-mail client is Microsoft's Outlook e-mail client and said analyser is a Microsoft Exchange client extension.

351. The method of claim 329 wherein said network comprises a server and said analyser is located at a point on said network intermediate said one or more workstations and said server, or said analyser is located at said server.

352. The method of claim 329 wherein said computer network to which said one or more workstations are adapted for connection is a public computer network,

and wherein said one or more workstations together form a private computer network.

353. The method of claim 329 further comprising the step of providing a supervisor workstation, said policy data being accessible by said supervisor workstation, such that a user of said supervisor workstation can edit said policy data.

354. A computer program product, for controlling a computer to manage information, said computer being connected to a public network and having access to policy data containing rules for the transmission to the public network of outbound data that may be part of a transaction, comprising:

a recording medium readable by the computer, having program code recorded thereon which when executed on said computer configures the computer to:

analyse, in conjunction with an application running on the computer that is operable to transmit outbound data to the public network and receive inbound data from the public network, at least said outbound data to identify, with reference to said rules of said policy data, transaction data that may be part of a transaction to determine, in accordance with said rules of said policy data, whether the transmission of said transaction data would satisfy said rules; and

to control the computer to control the transmission of said transaction data by said application in dependence on the determination made by said analyser.

355. The computer program product of claim 354 wherein said program code when executed on said computer is operable to control the computer such that said transaction data is either, transmitted, not transmitted, or sent to an approver who determines whether or not to transmit the transaction data.

356. The computer program product of claim 355 wherein the program code when executed on said computer is further operable to identify in said data that may be part of a transaction, data that needs approval; refer said data that needs approval to one or more approvers for approval, and monitor whether or not approval is received from said one or more approvers; and wherein the transmission of said transaction data by said application depends on whether or not approval is received from said one or more approvers;

357. The computer program product of claim 356 wherein said program code when executed on said computer is further operable to identify said transaction data that needs approval by determining the nature of said transaction data and checking said rules of said policy data, said rules of said policy data defining whether or not approval is needed in dependence on the determined nature of said transaction data.

358. The computer program product of claim 356 wherein said program code when executed on said computer is further operable to determine the nature of said transaction data by identifying at least one of the identity of the transmitter of said data, the identity of the intended recipient of said data, the computer in the private network from which said data is to be transmitted, the sum for which a transaction is to be made, and the account from which a transaction is to be made.

359. The computer program product of claim 356 wherein said program code when executed on said computer is further operable to determine the nature of said transaction data that needs approval and select

said one of said one or more approvers in dependence on that determination.

360. The computer program product of claim 359 wherein said program code when executed on said computer is operable to determine the nature of said transaction data that needs approval by identifying at least one of the identity of the transmitter of said data, the identity of the intended recipient of said data, the computer in the private network from which said data is to be transmitted, the sum for which a transaction is to be made, and the account from which the transaction is to be made.

361. The computer program product of claim 354 wherein said program code when executed on said computer is operable to determine whether a secure link has been negotiated between said application and a remote site on said public network, and to identify said outbound data or said inbound data as transaction data, if it is transmitted on a secure link.

362. The computer program product of claim 361 wherein said public network is the Internet, and said rules of said policy data define the addresses of web sites or e-mail accounts that negotiate secure links for the transmission of data but which are known not to be eCommerce sites or accounts, and said program code when executed on said computer is operable to disregard said outbound data transmitted to those web sites or accounts or said inbound data received from those web sites or accounts, such that no approval is required.

363. The computer program product of claim 354 wherein said program code when executed on said computer is operable to identify transaction data by reference to said rules of said policy data, said rules

of said policy data defining the addresses of known eCommerce web sites and the e-mail accounts.

364. The computer program product of claim 354 wherein said program code when executed on said computer is operable to identify credit card numbers in said outbound data or said inbound data, and to identify outbound data or inbound data that contains a credit card number as transaction data.

365. The computer program product of claim 364 wherein said policy data specifies pre-determined credit card numbers that can never be transmitted.

366. The computer program product of claim 354 wherein said program code when executed on said computer is operable to identify transaction data by reference to said rules of said policy data, said rules of said policy data defining one or more of pre-determined digital certificates, account codes, pre-determined keywords, pre-determined names and addresses and embedded codes.

367. The computer program product of claim 354 wherein said program code when executed on said computer is operable to detect an embedded code in said inbound data, said embedded code having been placed in said inbound data to mark said inbound data as transaction data.

368. The computer program product of claim 354 further comprising, a selector, recorded on said recording medium, said selector being operable to select data in said outbound and said inbound data that is part of a transaction in response to input from a user, said program code when executed on said computer being operable to identify said outbound and said inbound data so selected.

369. The computer program product of claim 354 wherein said program code is executable at said computer.

370. The computer program product of claim 354 wherein said application is a web browser.

371. The computer program product of claim 370 wherein said program code when executed on said computer is a plug-in module of said web browser.

372. The computer program product of claim 371 wherein said web browser is Microsoft's Internet Explorer and said plug-in module is a Browser Helper Object.

373. The computer program product of claim 354 wherein said application is an e-mail client.

374. The computer program product of claim 373 wherein said program code when executed on said computer is a plug-in module of said e-mail client.

375. The computer program product of claim 374 wherein said e-mail client is Microsoft's Outlook e-mail client and said plug-in module is a Microsoft Exchange client extension.

376. The computer program product of claim 354 wherein said public network includes a server and said program code is executable at a point on said network intermediate said computer and said server, or said program code is executable at said server.

377. An information management system comprising:

one or more workstations adapted for connection to a computer network, each workstation having a memory;

an application stored in said memory of each workstation for receiving at least inbound data from said network;

an analyser, said analyser being operable in conjunction with said application to monitor said inbound data and to identify in at least said inbound data, signed data that has been digitally signed with a digital certificate, to extract one or more details of said signed data and to determine whether or not verification is required for said digital certificate;

policy data, accessible by said analyser, containing rules which define whether or not verification is required for said digital certificate;

and wherein said analyser determines whether or not verification is required for said digital certificate in dependence on said rules of said policy data and in dependence on said one or more details of said signed data extracted by said analyser.

378. The system of claim 377 wherein said verification for said digital certificate includes determining whether said digital certificate has been revoked.

379. The system of claim 378 wherein said analyser is further operable to determine whether said signed data is part of an eCommerce transaction, and if it is, to determine the amount of money that is promised in that eCommerce transaction,

wherein said verification for the digital certificate also includes determining whether said digital certificate can be taken as a guarantee of receiving the amount of money promised in said eCommerce transaction.

380. The system of claim 377 wherein said analyser is operable to extract as one or more details of said signed data, one or more of said digital certificate holder's identity, the expiry date of said digital certificate, the issue number of said digital certificate, and the domain name from which the signed data was received, and wherein said rules of said policy file define whether or not verification for said digital certificate is required in dependence on the one or more details extracted by said analyser.

381. The system of claim 377 wherein said analyser is operable to determine whether or not an eCommerce transaction is occurring, and to extract, as one or more details of said signed data, the amount of any transaction being made with said digital certificate, the account code from which any payment is being made, a credit card number, one or more indicators of the nature of the transaction, and wherein said rules of said policy file define whether or not verification is required for a digital certificate in dependence on the one or more details extracted by said analyser.

382. The system of claim 381 further comprising a data repository in which, digital certificates used to digitally sign any previously received signed data or sufficient decriptive data to identify any such digital certificates, and transaction data describing any previous transactions made with those digital certificates are stored,

said transaction data being at least one or more of the date of any previous transactions made with a digital certificate, and the amount of any previous transaction made with that digital certificate,

and wherein said rules of said policy file define whether or not verification for said digital certificate is required in dependence on said transaction data.

383. The system of claim 377 further comprising a data repository, accessible by said analyser, wherein said analyser is operable to identify any digital certificates that are used to digitally sign signed data in at least said inbound data, and to cause any such digital certificates, or sufficient descriptive data to identify such digital certificates to be stored in said data repository.

384. The system of claim 383 wherein said analyser is operable, to record the results of any verification for an digital certificate in said data repository together with said digital certificate or together with said descriptive data.

385. The system of claim 384 wherein said analyser is operable, if it identifies a digital certificate in said inbound data, to determine whether said digital certificate has been previously stored in said data repository, or whether said descriptive information identifying said digital certificate has been stored in said data repository, and if said digital certificate has been previously stored, to look-up the results of any previous verification of whether said digital certificate has been revoked, wherein said analyser determines whether or not to verify if said digital certificate has been revoked in dependence on said results of any previous verification of whether said identified digital certificate has been revoked.

386. The system of claim 377 wherein said analyser is further operable to verify whether or not a digital certificate has been revoked, and wherein said application is operable to prevent said inbound data being viewed by a user of said application if said analyser determines that said digital certificate has been revoked.

387. The system of claim 377 wherein said analyser is further operable to verify whether or not a digital certificate has been revoked, and said application is operable to notify a user of said application that said inbound data is not to be relied upon if said analyser determines that said digital certificate has been revoked.

388. The system of claim 377 wherein said analyser is located on each of said one or more workstations.

389. The system of claim 377 wherein said application is a web browser.

390. The system of claim 389 wherein said analyser is a plug-in module of said web browser.

391. The system of claim 390 wherein said web browser is Microsoft's Internet Explorer and said analyser is a Browser Helper Object.

392. The system of claim 377 wherein said application is an e-mail client.

393. The system of claim 392 wherein said analyser is a plug-in module of said e-mail client.

394. The system of claim 393 wherein said e-mail client is Microsoft's Outlook e-mail client and said analyser is a Microsoft client extension.

395. The system of 377 wherein said network comprises a server, and said analyser is located at a point on said network intermediate said one or more workstations and said server, or said analyser is located at said server.

396. The system of claim 377 wherein said computer network to which said one or more workstations are adapted for connection is a public computer network, and wherein said one or more workstations together form a private computer network.

397. The system of claim 377 further comprising a supervisor workstation, said policy data being accessible by said supervisor workstation, such that a user of said supervisor workstation can edit said policy data.

398. A method of managing information comprising the steps of:

providing one or more workstations adapted for connection to a computer network, each workstation having a memory;

providing an application stored in said memory of each workstation for receiving at least inbound data from said network;

providing policy data, containing rules which define whether or not verification is required for a digital certificates used to digitally sign signed data received in said inbound data;

identifying in at least said inbound data, signed data that has been digitally signed with a digital certificate;

extracting one or more details of said signed data; and

determining whether or not verification is required for said digital certificate in dependence on said rules of said policy data and in dependence on said one or more details of said signed data extracted in said extracting step.

399. The method of claim 398 wherein said verification for the digital certificate includes

determining whether the digital certificate has been revoked.

400. The method of claim 399 further comprising the step of determining whether said signed data is part of an eCommerce transaction, and if it is, determining the amount of money that is promised in that eCommerce transaction,

wherein said verification for the digital certificate also includes determining whether said digital certificate can be taken as a guarantee of receiving the amount of money promised in said eCommerce transaction.

401. The method of claim 398 wherein said one or more details of said signed data extracted in said extracting step, include one or more of said digital certificate holder's identity, the expiry date of said digital certificate, the issue number of said digital certificate, and the domain name from which the signed data was received, and wherein said rules of said policy file define whether or not verification for said digital certificate is required in dependence on the one or more details.

402. The method of claim 398 further comprising the step of determining whether or not an eCommerce transaction is occurring, and if it is, extracting in said extracting step, as one or more details of said inbound data, the amount of any transaction being made with said digital certificate, the account code from which any payment is being made, a credit card number, one or more indicators of the nature of the transaction, and wherein said rules of said policy file define whether or not verification is required for a digital certificate in dependence on said one or more details.

403. The method of claim 402 further comprising the step of providing a data repository in which digital certificates used to digitally sign any previously received signed data or sufficient descriptive data to identify any such digital certificates, and transaction data describing any previous transactions made with those digital certificates are stored;

said transaction data being at least one or more of the date of any transactions made with a digital certificate, and the amount of any transaction made with that digital certificate,

and wherein said rules of said policy file define whether or not verification for said digital certificate is required in dependence on said transaction data.

404. The method of claim 398 further comprising the steps of identifying digital certificates used to sign signed data in said inbound data or digital certificates transmitted in said inbound data and storing said digital certificates or sufficient descriptive data to identify said digital certificates in said data repository.

405. The method of claim 404 further comprising the steps of recording the results of any verification for an digital certificate in said data repository together with said digital certificate.

406. The method of claim 405 further comprising the step of determining whether said digital certificate has been previously stored in said data repository, and if it has been previously stored, to look-up the results of any previous verification for said digital certificate,

wherein said step of determining whether or not verification is required for said digital

certificate is dependent on said results of any previous verification for said digital certificate.

407. The method of claim 398 further comprising the steps of determining whether or not a digital certificate has been revoked, and preventing said inbound data being viewed by a user of said application if said identified digital certificate has been revoked.

408. The method of claim 398 further comprising the steps of determining whether or not a digital certificate has been revoked, and notifying a user of said application that said inbound data is not to be relied upon if said digital certificate has been revoked.

409. The method of claim 398 wherein said steps of identifying a digital certificate, extracting one or more details from said signed data and determining whether or not verification is required are performed at said one or more workstations.

410. The method of claim 398 wherein said application is a web browser.

411. The method of claim 410 wherein said steps of identifying a digital certificate, extracting one or more details from said signed data and determining whether or not verification is required are performed by a plug-in module of said web browser.

412. The method of claim 411 wherein said web browser is Microsoft's Internet Explorer and said plug-in module is a Browser Helper Object.

413. The method of claim 398 wherein said application is an e-mail client.

414. The method of claim 413 wherein said steps of identifying a digital certificate, extracting one or more details from said signed data and determining whether or not verification is required are performed by a plug-in module of said e-mail client.

415. The method of claim 416 wherein said e-mail client is Microsoft's Outlook e-mail client and said plug-in module is a Microsoft Exchange client extension.

416. The method of claim 398 wherein said network comprises a server, and said steps of identifying a digital certificate, extracting one or more details from said signed data and determining whether or not verification is required are performed at a point on said network intermediate said one or more workstations and said server, or said steps of identifying a digital certificate, extracting one or more details from said signed data and determining whether or not verification is required are performed at said server.

417. The method of claim 398 wherein said computer network to which said one or more workstations are adapted for connection is a public computer network, and wherein said one or more workstations together form a private computer network.

418. The method of claim 398 further comprising providing a supervisor workstation, said policy data being accessible by said supervisor workstation, such that a user of said supervisor workstation can edit said policy data.

419. A computer program product for controlling a computer connected to a public network to manage information, said computer having access to policy data

containing rules which define whether or not verification is required for a digital certificate used to digitally sign signed data received in inbound data from the public network,

comprising:

a recordable medium readable by the computer, having program code recorded thereon which when executed on said computer configures said computer to:

analyse, in conjunction with an application running on the computer that is operable to receive at least inbound data from the public network, signed data that has been digitally signed with a digital certificate, to extract one or more details of said signed data;

to determine whether or not verification is required for said digital certificate in dependence on said rules of said policy data and in dependence on the one or more extracted details of said signed data; and

to control the application in dependence on the determination.

420. The computer program product of claim 419 wherein said verification for the digital certificate includes determining whether the digital certificate has been revoked.

421. The computer program product of claim 420 wherein said program code when executed on said computer is further operable to determine whether said signed data is part of an eCommerce transaction, and if it is, to determine the amount of money that is promised in that eCommerce transaction,

wherein said verification for the digital certificate also includes determining whether said digital certificate can be taken as a guarantee of receiving the amount of money promised in said eCommerce transaction.

422. The computer program product of claim 419 wherein said one or more details of said signed data, include one or more of said digital certificate holder's identity, the expiry date of said digital certificate, the issue number of said digital certificate, and the domain name from which the signed data was received, and wherein said rules of said policy file define whether or not verification for said digital certificate is required in dependence on the one or more details.

423. The computer program product of claim 419 wherein said program code when executed on said computer is further operable to determine whether or not an eCommerce transaction is occurring, and if it is, to extract as one or more details of said signed data, the amount of any transaction being made with said digital certificate, the account code from which any payment is being made, a credit card number, one or more indicators of the nature of the transaction, and wherein said rules of said policy file define whether or not verification is required for said digital certificate in dependence on said one or more details.

424. The computer program product of claim 423 wherein the program code when executed on said computer is further operable to control the computer to record digital certificates used to digitally sign any signed data received in said inbound data or sufficient descriptive data to identify any such digital certificates, and transaction data describing any transactions made with those digital certificates in a data repository such that a record is maintained of transactions made with a digital certificate;

said transaction data being at least one or more of the date of any transactions made with a digital certificate, and the amount of any transaction made with that digital certificate,

and wherein said rules of said policy file define whether or not verification for said digital certificate is required in dependence on said transaction data.

425. The computer program product of claim 419 wherein said program code when executed on said computer is further operable to control the computer to store digital certificates used to sign signed data in said inbound data or digital certificates transmitted in said inbound data and storing said digital certificates or sufficient descriptive data to identify said digital certificates in a data repository.

426. The computer program product of claim 425 wherein said program code when executed on said computer is further operable control the computer to record the results of any verification for an identified digital certificate in said data repository together with said identified digital certificate.

427. The computer program product of claim 426 wherein said program code when executed on said computer is operable to determine whether said identified digital certificate has been previously stored in said data repository, and if it has been previously stored, to look-up the results of any previous verification for said identified digital certificate,

wherein the determination of whether or not verification is required for said identified digital certificate is dependent on said results of any previous verification for said identified digital certificate.

428. The computer program product of claim 419 wherein said program code when executed on said computer is operable to determine whether or not a

digital certificate has been revoked, and control said application to prevent said inbound data being viewed by a user of said application if said identified digital certificate has been revoked.

429. The computer program product of claim 419 wherein said program code when executed on said computer is operable to determine whether or not a digital certificate has been revoked, and to control said application to notify a user of said application that said inbound data is not to be relied upon if said identified digital certificate has been revoked.

430. The computer program product of claim 419 wherein said program code is executable at said computer.

431. The computer program product of claim 419 wherein said application is a web browser.

432. The computer program product of claim 431 wherein said program code when executed on said computer is a plug-in module of said web browser.

433. The computer program product of claim 432 wherein said web browser is Microsoft's Internet Explorer and said plug-in module is a Browser Helper Object.

434. The computer program product of claim 419 wherein said application is an e-mail client.

435. The computer program product of claim 434 wherein said program code when executed on said computer is a plug-in module of said e-mail client.

436. The computer program product of claim 435 wherein said e-mail client is Microsoft's Outlook e-

mail client and said plug-in module is a Microsoft Exchange client extension.

437. The computer program product of claim 419 wherein said network includes a server and said program code is executable at a point on said network intermediate said computer and said server, or said program code is executable at said server.